UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ADAM MCAFEE, individually and on behalf of all others similarly situated, Plaintiff, v. COINBASE, INC. and COINBASE GLOBAL, INC., Defendants.	Case No. 1:25-cv-4137 **CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiff Adam McAfee, by and through his undersigned counsel, files this Class Action Complaint individually and on behalf of a class of all similarly situated persons against Defendants Coinbase, Inc. and Coinbase Global, Inc. (collectively, "Coinbase" or "Defendants"). Plaintiff bases the following allegations upon information and belief, investigation of counsel, and their own personal knowledge.

I. NATURE OF THE ACTION

1. Plaintiff brings this action against Coinbase for their failure to properly secure and safeguard highly valuable, protected, personally identifiable information including, *inter alia*, names, addresses, phone numbers, emails, the last four digits of Social Security numbers, masked bank-account numbers and some bank account identifiers, Government-ID images (*e.g.*, driver's license, passport), account data (such as balance snapshots and transaction history), and limited corporate data (including documents, training material, and communications available to support agents) (collectively, "PII"); and for their failure to comply with industry standards to protect information systems that contain PII.[1]

[1] *Form 8-K*, Coinbase Global, Inc. (May 14, 2025), https://www.sec.gov/Archives/edgar/data/1679788/000167978825000094/coin-20250514.htm#:~:text=On%20May%2011%2C%202025%2C%20Coinbase%2C%20Inc.

2. Coinbase is a cryptocurrency exchange with a quarterly trading volume of $393 billion. Coinbase's mission is to "increase economic freedom for more than 1 billion people."[2]

3. In order to obtain Defendants' services, Coinbase's customers are required to directly or indirectly entrust Coinbase with their PII, which Coinbase uses in order to perform their regular business services.

4. As a cryptocurrency exchange, Coinbase therefore knowingly collects and stores sensitive PII of their customers, and has a resulting duty to secure such information from unauthorized access and exfiltration.

5. Coinbase expressly recognizes these duties, representing that "We at Coinbase respect and protect the privacy of those who explore our Services."[3]

6. Despite their duties to safeguard individuals' PII, on May 11, 2025, Coinbase became aware of a cybersecurity incident as Coinbase received an email communication from an unknown threat actor claiming to have obtained information about certain Coinbase customer accounts, as well as internal Coinbase documentation, including materials relating to customer-service and account-management systems. The communication demanded ransom in exchange for not publicly disclosing the information. The threat actor appears to have obtained this information by paying multiple contractors or employees working in support roles outside the United States to collect information from internal Coinbase systems (the "Data Breach" or "Breach").[4]

7. As a direct and proximate result of Coinbase's negligent failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII—names, addresses, phone

[2] *About Coinbase*, coinbase, https://www.coinbase.com/about (last visited May 16, 2025).
[3] *Coinbase Global Privacy Policy*, coinbase (last updated March 26, 2024), https://www.coinbase.com/legal/privacy.
[4] *Form 8-K, supra* note 1.

numbers, emails, the last four digits of Social Security numbers, masked bank-account numbers and some bank account identifiers, Government-ID images (*e.g.*, driver's license, passport), account data (such as balance snapshots and transaction history), and limited corporate data (including documents, training material, and communications available to support agents)—is now in the hands of cybercriminals.

8. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, and other harms caused by the unauthorized disclosure of their PII—risks which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

9. Plaintiff brings claims for negligence, negligence *per se*, unjust enrichment, and declaratory judgment, seeking damages and injunctive relief, including the adoption of reasonably sufficient data security practices to safeguard the PII in Defendants' possession in order to prevent incidents like the Data Breach from reoccurring in the future.

II. PARTIES

10. Plaintiff Adam McAfee, at all relevant times, is and was a citizen of the State of California. Plaintiff utilizes Defendants' cryptocurrency exchange.

11. Defendant Coinbase, Inc. is a is a Delaware corporation with a principal place of business located at One Madison Avenue, Suite 2400, New York, New York 10016.[5]

[5] When subject matter jurisdiction is established under the Class Action Fairness Act, "an LLC's citizenship is based on its principal place of business and laws of incorporation." *Hernandez v. Pure Health Rsch. LLC*, No. 23-cv-00971, 2023 U.S. Dist. LEXIS 191909, at *7 (S.D. Cal. Oct. 25, 2023) (applying § 1332(d)(10) of CAFA) (citing *Jack v. Ring LLC*, 553 F. Supp. 3d 711, 715 (N.D. Cal. 2021)); *see also Abrego v. Dow Chem. Co*., 443 F.3d 676, 684 (9th Cir. 2006) (noting that § 1332(d)(10) of CAFA provides a different rule for unincorporated associations).

12. Defendant Coinbase Global, Inc. is a Delaware corporation with a principal place of business located at One Madison Avenue, Suite 2400, New York, New York 10016.

III. JURISDICTION AND VENUE

13. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, because Plaintiff and at least one member of the Class, as defined below, are citizens of a different state than Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

14. This Court has general personal jurisdiction over Defendants because Coinbase is a citizen of the State of New York.

15. This Court is the proper venue for this action pursuant to 28 U.S.C. § 1391(b)(1), because Defendants reside in this District, a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District; and Defendants conduct substantial business within this District.

IV. FACTUAL BACKGROUND

A. Coinbase Provides Cryptocurreny Exchange Services Involving Highly Sensitive Data.

16. Coinbase is "the most trusted place for people and businesses to buy, sell, and use crypto."[6]

17. Coinbase allows their customers to trade cryptocurrency by providing "a trusted platform that makes it easy for people and institutions to engage with crypto assets, including trading, staking, safekeeping, spending, and fast, free global transfers."[7]

[6] *Coinbase*, coinbase, https://www.coinbase.com/ (last visited May 16, 2025).
[7] *About Coinbase*, *supra* n. 2.

18. As part of providing their services, Coinbase is entrusted with their customers' PII. This sensitive PII includes but is not limited to, *inter alia*, names, addresses, phone numbers, emails, the last four digits of Social Security numbers, masked bank-account numbers and some bank account identifiers, Government-ID images (*e.g.*, driver's license, passport), account data (such as balance snapshots and transaction history), and limited corporate data (including documents, training material, and communications available to support agents).

19. When entrusting Coinbase with their PII, Plaintiff and Class Members reasonably expect Defendants would use the utmost care to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

20. Plaintiff and Class Members had a reasonable expectation, based in part on Coinbase's own statements, that their PII would be protected. Coinbase represents that "[t]rust is built on dependable security and protections—which is why we make protecting your account & your digital assets our number one priority."[8]

21. However, despite Defendants' stated commitment to data security, Coinbase failed to adopt reasonable measures to prevent the unauthorized access to Plaintiff's and Class Members' PII by unauthorized bad actors.

B. The Data Breach.

22. On or about May 11, 2025, Coinbase became aware of a potential cybersecurity incident as Coinbase received an email communication from an unknown threat actor claiming to have obtained information about certain Coinbase customer accounts, as well as internal Coinbase

[8] Gary Shambat, Identity verification and financial compliance, coinbase (March 31, 2023), https://www.coinbase.com/blog/identity-verification-and-financial-compliance.

documentation, including materials relating to customer-service and account-management systems.[9]

23. A threat actor reportedly targeted Coinbase's customer support agents overseas and used cash offers to convince a small group of insiders to copy data in their customer support tools for less than 1% of Coinbase monthly transacting users with the aim of gathering a customer list they could contact while pretending to be Coinbase—tricking people into handing over their cryptocurrency.[10]

24. The threat actor then demanded a $20 million ransom not to publish the stolen information. Defendants said they would not pay the ransom but would establish a $20 million reward fund for any leads that could help find the attackers who coordinated this attack.[11]

25. But even if Defendants took steps to ensure the data's deletion, *i.e.*, paid the threat actors a likely ransom to ensure the stolen information's destruction, criminals have no incentive to destroy such valuable information that may be monetized in the future, either through extracting additional ransom payments, or using the data to commit fraud and identity theft. As cybersecurity professional Brian Krebs has noted:

> Companies hit by ransomware often face a dual threat: Even if they avoid paying the ransom and can restore things from scratch, about half the time the attackers also threaten to release sensitive stolen data unless the victim pays for a promise to have the data deleted. Leaving aside the notion that victims might have any real expectation the attackers will actually destroy the stolen data, new research suggests a fair number of victims who do pay up may see some or all of the stolen data published anyway.[12]

---

[9] *Form 8-K*, *supra*, n. 1.

[10] *Protecting Our Customers - Standing Up to Extortionists*, coinbase (May 15, 2025), https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists.

[11] *Sergiu Gatlan*, *Coinbase data breach exposes customer info and government IDs*, BleepingComputer (May 15, 2025), https://www.bleepingcomputer.com/news/security/coinbase-discloses-breach-faces-up-to-400-million-in-losses/.

[12] Brian Krebs, *Why Paying to Delete Stolen Data is Bonkers*, Krebs on Security (Nov. 20, 2020), https://krebsonsecurity.com/2020/11/why-paying-to-delete-stolen-data-is-bonkers/.

26. Indeed, Coinbase cannot reasonably maintain the stolen information would be destroyed and will not be further disseminated. Defendants' own notice to impacted individuals advises them to remain vigilant for scammers and take further actions such enabling heightened security settings.[13]

27. The impacted information includes names, addresses, phone numbers, emails, the last four digits of Social Security numbers, masked bank-account numbers and some bank account identifiers, Government-ID images (*e.g.*, driver's license, passport), account data (such as balance snapshots and transaction history), and limited corporate data (including documents, training material, and communications available to support agents).[14]

28. Private assessments of the Data Breach indicate that Coinbase failed to implement basic steps to safeguard the PII that they were entrusted. After their own investigation, Coinbase discovered the threat actor gained access to Coinbase's customers' information by paying multiple contractors or employees working in support roles outside the United States to collect information from internal Coinbase systems to which they had access in order to perform their job responsibilities.[15]

29. On May 15, 2025, Coinbase reported the Data Breach to their customers that were affected by this incident.[16]

30. Upon information and belief, the Data Breach occurred as a direct and proximate result of Coinbase's intentional, willful, reckless, and/or negligent failure to implement and follow basic security procedures in order to protect their customers' PII. Indeed, had Coinbase properly

[13] *Protecting Our Customers*, *supra* n. 10.
[14] *Form 8-K*, *supra* n.1.
[15] *Id*.
[16] *Protecting Our Customers*, *supra* n. 10.

maintained and monitored their computer systems that stored the PII, Defendants would have discovered the Data Breach sooner rather than allowing the cybercriminals unimpeded access to access and exfiltrate Plaintiff's and Class Members' PII.

31. In any event, the scope of the Data Breach shows the severity of Coinbase's data security failings. The cybercriminals were able to gain access to Coinbase's customers' PII. If Coinbase had even minimal data security measures in place, they would have been able to detect the Data Breach at a point before cybercriminals were able to successfully obtain their customers' data.

C. The Value of Private Information and Effects of Unauthorized Disclosure.

32. Coinbase was well aware that the protected PII which they acquire is highly sensitive and of significant value to those who would use it for wrongful, nefarious purposes.

33. Coinbase also knew that a breach of their computer systems, and exposure of the PII therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

34. These risks are not theoretical, numerous high-profile breaches have occurred at companies such as Blackbaud, Fortra, Snowflake, Progress Software, Change Healthcare, and Accellion, amongst others, in recent years. These breaches put Defendants on notice that their electronic records would be targeted by cybercriminals.

35. PII is a valuable commodity to identity thieves. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[17] Indeed, a robust "cyber black market"

[17] *What To Know About Identity Theft*, FED. TRADE COMM'N CONSUMER ADVICE (Apr. 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited May 16, 2025).

exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the "dark web."

36. Criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the United States. In 2023, there were 6,077 recorded data breach incidents, exposing seventeen billion records. The United States specifically saw a 19.8% year-over-year increase in data breaches as compared to 2022.[18]

37. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[19]

38. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, credit and bank fraud, and more.

39. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of

[18] *2024 Global Threat Intelligence Report*, Flashpoint (Feb. 29, 2024), https://go.flashpoint.io/2024-global-threat-intelligence-report-download.

[19] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited May 16, 2024).

the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

40. The Social Security Administration even warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[20]

41. Social Security Numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

42. The ramifications of Coinbase's failure to keep Plaintiff's and Class Members' PII secure are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

[20] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

43. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[21]

44. Even if stolen PII and PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Indeed, even where cybercriminals do not gain access to a complete set of an individual's PII during a data breach, cybercriminals can cross-reference two or more sources of PII to marry data available elsewhere with criminally stolen data, resulting in complete and accurate dossiers on individuals. These dossiers are known as "Fullz" packages.

45. The development of Fullz packages means stolen PII from a data breach can easily be linked to victims' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information (such as emails, phone numbers, or credit card numbers) is not included in the PII stolen in a specific incident, criminals can easily create a Fullz package that links that information together and sell the package at a higher price.

46. Importantly, once a cybercriminal has a Fullz package, they can use it to commit a host of criminal acts including: credit card fraud, loan fraud, identity fraud, account take overs,

[21] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf.

medical identity fraud, tax refund fraud, and buy now pay later frauds.[22] Most problematic, however, is that cybercriminals in possession of a Fullz package "are difficult to stop with ordinary online security and ID verification measures because they possess all the information needed to get past typical authentication measures."[23]

47. A poll of security executives predicted an increase in attacks over the next two years from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[24]

48. Due to high-profile data breaches at other companies, Defendants knew or should have known that their customers' information would be targeted by cybercriminals.

49. Defendants also knew or should have known the importance of safeguarding the PII with which they were entrusted and of the foreseeable consequences if their data security systems were breached. Coinbase failed, however, to take adequate cybersecurity measures to prevent the Data Breach and the exfiltration of their customers' PII from occurring.

D. Coinbase Failed to Comply with FTC Guidelines and Industry Best Practices.

50. Coinbase is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data

[22] Paige Tester, *What Are Fullz? How Hackers and Fraudsters Obtain and Use Fullz*, DATADOME (Mar. 3, 2024), https://datadome.co/guides/account-takeover/what-are-fullz-how-do-fullz-work/.
[23] *Protection Against Fullz and Fraud*, INTEGRITY (Apr. 18, 2022), https://integrity.aristotle.com/2022/04/protection-against-fullz-and-fraud/.
[24] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*, FORBES (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864.

security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

51. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[25]

52. The FTC recommends that businesses:[26]

a. Identify all connections to the computers where sensitive information is stored;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

[25] *Start with Security: A Guide for Business*, U.S. Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 16, 2025).

[26] *Protecting Personal Information: A Guide for Business*, U.S. Federal Trade Comm'n (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 16, 2025).

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a

business's network, the transmission should be investigated to make sure it is authorized.

53. The FTC further recommends business take additional cybersecurity steps, which include:[27]

a. Conducting an inventory of all company devices that store sensitive data, and understanding what types of PII is stored on those devices;

b. Encrypting sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

c. Crafting a data security plan that involves both physical security (*e.g.*, locking up physical files) and electronic security, and training employees regarding the data security plan.

d. Promptly disposing of PII that is no longer needed, and retaining sensitive data only as long as companies maintain a legitimate business need for the information; and

e. Developing a plan to handle a data breach or data security incident, if and when such an incident occurs.

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

[27] *Id.*

55. Upon information and belief, Coinbase failed to properly implement one or more of the basic data security practices described above. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to PII resulted in the unauthorized access to and exfiltration of Plaintiff's and Class Members' PII.

56. Coinbase's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

57. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[28]

58. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[29] Upon information and belief, Coinbase failed to adhere to the NIST guidance.

59. Upon information and belief, Defendants' failure to protect Plaintiff's and Class Members' PII is a result of Coinbase's failure to adopt reasonable safeguards as required by the FTC, NIST, and industry best practices. This includes Coinbase's failure to enable multi-factor authentication on employee accounts, one of the most basic cybersecurity features.

[28] *See Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.
[29] *Id.* at Table 2 pg. 26-43.

60. Coinbase was, at all times, fully aware of their obligations to protect the PII of their customers because of their business model of collecting PII to provide their cryptocurrency exchange services. Coinbase was also aware of the significant repercussions that would result from their failure to do so.

E. Plaintiff and Class Members Suffered Damages.

61. The ramifications of Coinbase's failure to keep consumers' PII secure are long-lasting and severe. Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways, including theft of their PII as well as substantial and imminent risk of identity theft and fraud. Plaintiff and Class Members must immediately devote time, energy, and money to: (1) closely monitor their bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering, spear phishing, or extortion attacks; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

62. In 2019, the United States Government Accountability Office ("GAO") released a report addressing the steps consumers can take after a data breach.[30] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps data breach

[30] Government Accountability Off., *Data Breaches* (Mar. 2019), https://www.gao.gov/assets/gao-19-230.pdf (last visited May 16, 2025).

victims (like Plaintiff and Class Members) must take after a data breach, like Defendants', are both time-consuming and of only limited and short-term effectiveness.

63. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[31]

64. Coinbase recognizes the certainly impending and increased risk of identity theft and fraud that Plaintiff and Class Members now face as they have stated that they have implemented additional security measures for consumers to withdraw money from their accounts as well as heighted defenses against potential scammers.[32] Coinbase has further encouraged individuals "to remain vigilant against incidents of identity theft and fraud by reviewing account statements for suspicious activity."[33]

65. Further, once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse.

66. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when PIIs stolen and when it is used. According to the GAO, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

[31] *See Identity Theft Victim Checklist*, Fed. Trade Comm'n, https://www.identitytheft.gov/Steps (last visited May 16, 2025).
[32] *Protecting Our Customers*, *supra* n. 10.
[33] *Id.*

> continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[34]

67. For these reasons, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendants' conduct.

68. The value of Plaintiff's and Class Members' PII has been diminished by its exposure in the Data Breach. Indeed, PII is a valuable commodity to identity thieves, and, once it has been compromised, criminals will use them and trade the information on the cyber black market for years thereafter.[35]

69. The reality is that cybercriminals seek nefarious outcomes from a data breach, and stolen PII can be used to carry out a variety of crimes.

70. Plaintiff and Class Members are also at a continued risk because their information remains in Defendants' systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendants fail to undertake the necessary and appropriate security and training measures to protect their customers' PII.

71. As a result of Coinbase's failures, Plaintiff and Class Members face an increased risk of potential scams, identity theft and fraud, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim to cybercrimes for years to come.

72. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private information to strangers and cybercriminals.

---

[34] *See* 2007 GAO Report, at 29.

[35] *The Price Cybercriminals Charge for Stolen Data*, Trustwave (Aug. 6, 2023), https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-price-cybercriminals-charge-for-stolen-data/.

F. Plaintiff's Experience.

73. Plaintiff is a customer of Coinbase and exchanges cryptocurrency on their platform. In order to utilize Defendants' exchange, Plaintiff was required to entrust Coinbase with his PII. In collecting and maintaining the PII of Plaintiff, Defendants undertook a duty to act reasonably in their handling of Plaintiff's PII. Coinbase, however, did not take reasonable care of Plaintiff's PII, leading to its exposure and compromise as a direct result of Defendant's inadequate data security measures.

74. Plaintiff has started receiving spam calls and texts relating to his Coinbase account.

75. Since the announcement of the Data Breach, Plaintiff has been required to spend his valuable time and effort taking steps to avoid potential scams attempting to gain access to his account and mitigate the risk of misuse of his PII. Specifically, Plaintiff has been required to spend his valuable time and effort monitoring his Coinbase account and resetting passwords to his financial accounts. Plaintiff would not have had to engage in these time intensive efforts but for the Data Breach.

76. Plaintiff has suffered actual injury from having his PII exposed and/or stolen as a result of the Data Breach, including: (a) mitigation efforts to prevent scammers accessing his account; (b) mitigation efforts to prevent the misuse of his PII; (c) damages to and diminution of the value of his PII, a form of intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; and (d) loss of privacy.

77. Given the nature of the information compromised in the Data Breach and the propensity of criminals to use such information to commit a wide variety of crimes, Plaintiff faces

a significant, present, and ongoing risk of scams, identity theft and fraud, and other identity-related fraud now and into the indefinite future.

78. In addition, knowing that hackers gained access to his PII and that this information likely has been and will be used in the future for scams, identity theft, fraud, and other nefarious purposes has caused Plaintiff to experience significant frustration, anxiety, worry, stress, and fear.

V. CLASS ACTION ALLEGATIONS

79. Plaintiff, individually and on behalf of all others similarly situated, brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the class defined as:

> All individuals in the United States whose PII was compromised in the Coinbase Data Breach (the "Class").

80. Excluded from the Class are Defendants, their subsidiaries and affiliates, their officers, directors, and members of their officers' and directors' immediate families, any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of those judicial officers' immediate families.

81. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

82. **Numerosity.** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable

through Defendants' records, including, but not limited to, the files implicated in the Data Breach. Upon information and belief, the Class, at minimum, comprises over a million individuals.[36]

83. **Commonality.** This action involves questions of law and fact that are common to Plaintiff and the Class Members. Such common questions include, but are not limited to:

- Whether and to what extend Defendants had a duty to protect the PII of Plaintiff and Class Members;
- Whether Defendants were negligent in collecting and storing Plaintiff's and Class Members' PII;
- Whether Defendants had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
- Whether Defendants took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;
- Whether Defendants failed to adequately safeguard the PII of Plaintiff and Class Members;
- Whether Defendants breached their duties to exercise reasonable care in handling Plaintiff's and Class Members' PII;
- Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conduct; and

[36] Gatlan, *supra* n. 11.

- Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

84. **Typicality.** Plaintiff' claims are typical of the claims of the Class Members. The claims of Plaintiff and Class Members are based on the same legal theories and arise from the same failure by Defendants to safeguard their PII. Plaintiff and Class Members entrusted Defendants with their PII, and it was subsequently accessed by an unauthorized third party.

85. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

86. **Superiority.** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

87. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business

practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendants breached their duties and released Plaintiff's and Class Members' PII, then Plaintiff and each Class member suffered damages by that conduct.

88. **Ascertainability:** Members of the Class are ascertainable. Class Membership is defined using objective criteria, and Class Members may be readily identified through Defendants' books and records.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

89. Plaintiff restates and realleges the allegations contained in paragraphs 1 through 88 as if fully set forth herein.

90. Defendants owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

91. Specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendants' security systems to ensure that Plaintiff's and Class Members' PII in Defendants' possession was adequately secured and protected; (b) implementing processes that would detect a breach of their security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by their own security systems, regarding intrusions to their networks; and (d) maintaining data security measures consistent with industry standards.

92. Coinbase's duty to use reasonable care arose from several sources, including but not limited to those described below.

93. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendants. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Coinbase was obligated to act with reasonable care to protect against these foreseeable threats.

94. Defendants also owed a common law duty because their conduct created a foreseeable risk of harm to Plaintiff and Class Members. Coinbase's conduct included their failure to adequately restrict access to their computer networks and/or servers that held individuals' PII.

95. Defendants also knew or should have known of the inherent risk in collecting and storing massive amounts of PII, the importance of implementing adequate data security measures to protect that PII, and the frequency of cyberattacks such as the Data Breach in the financial sector.

96. Defendants breached the duties owed to Plaintiff and Class Members and thus was negligent. Coinbase breached these duties by, among other things: (a) mismanaging their system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; (f) failing to detect the

breach at the time it began or within a reasonable time thereafter; (g) failing to follow their own privacy policies provided to customers; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

97. But for Coinbase's wrongful and negligent breach of their duties owed to Plaintiff and Class Members, their PII would not have been access, exfiltrated, and compromised by cybercriminals.

98. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered injuries including:

a. Theft of their PII;

b. Costs associated with requesting credit freezes;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. Damages to and diminution in value of their PII entrusted to Coinbase with the mutual understanding that Defendants would safeguard Plaintiff' and

Class Members' data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members.

99. As a direct and proximate result of Coinbase's negligence, including their gross negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION

NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

100. Plaintiff restates and realleges the allegations contained in paragraphs 1 through 88 as if fully set forth herein.

101. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Coinbase for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duties.

102. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect customers' PII and not complying with the industry standards. Coinbase's conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of a data breach.

103. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

104. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

105. Coinbase's violation of Section 5 of the FTC Act constitutes negligence *per se*.

106. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered injuries, including those identified in paragraph 99 above.

107. As a direct and proximate result of Coinbase's negligence, Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

108. Plaintiff restates and realleges the allegations contained in paragraphs 1 through 88 as if fully set forth herein.

109. Plaintiff and Class Members conferred a monetary benefit on Coinbase by providing them with their valuable PII.

110. Coinbase knew that Plaintiff and Class Members conferred a benefit upon them and accepted and retained that benefit by accepting and retaining the PII entrusted to them. Defendants profited from Plaintiff's and Class Members' PII and use of Plaintiff's and Class Members' PII for business purposes.

111. Defendants failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

112. Coinbase acquired the PII through inequitable record retention as they failed to disclose the inadequate data security practices previously alleged.

113. If Plaintiff and Class Members had known Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would not have agreed to the entrustment of their PII to Defendants.

114. Under the circumstances, it would be unjust for Coinbase to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon them.

115. Plaintiff and Class Members are without an adequate remedy at law.

116. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered injuries, including those identified in paragraph 98 above.

117. Plaintiff and Class Members are entitled to restitution and/or damages from Coinbase and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct, as well as return of their sensitive PII and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

FOURTHCAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

118. Plaintiff restates and realleges the allegations contained in paragraphs 1 through 88 as if fully set forth herein.

119. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described herein.

120. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Coinbase is currently maintaining data security

measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendants still possess Plaintiff's and Class Members' PII, and that Defendants' data security measures remain inadequate. Furthermore, Plaintiff and Class Members continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

121. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure consumers' PII under the common law and Section 5 of the FTC Act; and

b. Defendants continue to breach this legal duty by failing to employ reasonable data security measures to safeguard Plaintiff's and Class Members' PII.

122. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect consumers' PII in their possession.

123. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Coinbase. The risk of another such breach is real, immediate, and substantial. If another breach at Coinbase occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

124. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants

of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

125. Issuance of the requested injunction will not disserve the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, prays for relief as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representatives of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. For damages in an amount to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiff' reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; and

H. Awarding such other and further relief as may be just and proper.

VIII. JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: May 16, 2025

LYNCH CARPENTER, LLP

/s/ Gary F. Lynch
Gary F. Lynch (NY 5553854)
gary@lcllp.com
Nicholas A. Colella (*pro hac vice* forthcoming)
nickc@lcllp.com
1133 Penn Ave., 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246

Attorneys for Plaintiff and the Proposed Class